UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/576,250	04/18/2006	Stefano Brusotti	09952.0027-00000	8838

22852 7590 04/20/2010

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
PHAM, LUU T	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
04/20/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/576,250	BRUSOTTI ET AL.	
	Examiner	Art Unit	
	LUU PHAM	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01/27/2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *37-72* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *37-72* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the Amendment filed on 01/27/2010.

2. In the instant Amendment, Claims 1-36 were previously cancelled; claims 37, 54, and 72 have been amended; Claims 37-72 have been examined and are pending.

This Action is made FINAL.

Response to Arguments

3. The objection to the abstract is withdrawn as the abstract has been amended.

4. The rejections of claims 37-51 under 35 U.S.C. § 101 are withdrawn as Applicants' arguments have found persuasive.

5. The rejection of claim 72 under 35 U.S.C. § 101 is maintained as the claim still directed to non-statutory subject matter. Applicants' arguments with respect to the statutory subject matter of claim 72 have been fully considered but they are not persuasive. Claim 72 recites *"[a] computer readable medium encoded with a program product;"* However, there is no further discussion in the specification as to what type of computer readable storage medium is claimed. Broadly interpreted, a *"computer-readable medium"* can be any means that include propagate and transmission signals, which are non-eligible subject matter under 35 U.S.C. 101; Therefore, the claims are directed to non-statutory subject matter. Please refer to sections 7 and 8, Claim Rejections - 35 USC § 101, below for further details.

6. Applicants' arguments in the instant Amendment, filed on 01/27/2010, have been fully considered but they are not persuasive.

Applicants' arguments:

a. *Baehr does not disclose or suggest at least Applicants' claimed 'in the absence of an adverse effect, allowing, by said test system, the communication entities not having the adverse effect to communicate with said set of machines,' as recited in claim 37 (and similarly in claim 54)."*

b. *"The Office Action* appears *to equates the 'proxy network' of Baehr with the 'test system' of claim 37. See id. This is incorrect. The 'test system' of claim 37 and the 'proxy network' of Baehr are distinguishable."*

The Examiner disagrees for the following reasons:

a. Baehr does disclose in the absence of an adverse effect, allowing, by said test system, the communication entities not having the adverse effect to communicate with said set of machines *(col. 6, lines 50-59; if it does, this is an indication that intruder may be attempting to breach the private network by masquerading as a trusted hot; in this case, the screen 340 should drop the packet without reply [otherwise, the screen will not drop the packet (forwarding the packet to destination)]; col. 7, lines 16-21; col. 7, lines 39-43; col. 10, lines 19-34; Fig. 11; steps 990: 'create connection' and 1010: 'check connection').*

b. As addressed in section 6 of the Office Action, mailed on 10/27/2009, the screening system 340, which includes proxy network 445, could be equated with the 'test system' claimed by the Applicants because the proxy network includes a virtual host mirroring (or acting as proxy for) each of a subset (or all) of the hosts

found on the private network 330; the proxy hosts are 'virtual' in the sense that they are not the actual targeted host 360-380, but rather mimic the behavior of the those hosts *(col. 2, lines 25-30; col. 4, lines 27-40; col. 4, lines 50-63).*

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. **Claim 72 is rejected under 35 U.S.C. 101** as being directed to non-statutory subject matter.

- **Regarding claim 72**, claim 72 is rejected under 35 U.S.C. 101 because the claim is directed to non-statutory subject matter. Claim 72 recites *"[a] computer readable medium encoded with a program product;"* However, there is no further discussion in the specification as to what type of computer readable storage medium is claimed. Broadly interpreted, a *"computer-readable medium"* can be any means that include propagate and transmission signals, which are non-eligible subject matter under 35 U.S.C. 101; Therefore, the claims are directed to non-statutory subject matter. The Examiner respectfully suggests that the claims be amended as *"A* ***non-transitory*** *computer readable storage medium"* to make the claim statutory under 35 USC 101; (emphasis added).

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

10. **Claims 37-39, 46-51, 54-56, 63-68, and 71-72 are rejected under 35 U.S.C. 102(b)** as being anticipated by Baehr et al., (hereinafter "Baehr"), U.S. Patent No. 5,878,231, issued on March 02, 1999.

- **Regarding claim 37**, Baehr discloses a method of preventing intrusion in communication traffic with a set of machines in a network, said traffic comprising communication entities *(col. 3, lines 16-50; Figs. 4-6; proxy network 430; col. 4, lines 64-67; Fig. 7; proxy network 445 implemented on screening system 340)*, comprising the steps of:

providing a test system comprising test facilities replicating at least one of said machines in said set *(col. 4, lines 27-40; col. 4, lines 50-63; Figs. 5-6; proxy network 430/445 includes a virtual host mirroring (or acting as proxy for) each of a subset (or all) of the hosts found on the private network 330; col. 4, lines 64-67; Fig. 7; screening system 340, which includes proxy network 445, is known as test system)*;

directing at least part of said communication entities in said traffic toward said test system *(col. 2, lines 25-36; col. 4, lines 57-60; Figs. 4-7; when a user attempts to access a service or host of the private network, the request may be shunted aside to the*

proxy network to either a mirroring proxy host or a unique proxy host; see also col. 6, lines 30-36);

running said communication entities directed toward said test system on said test facilities to detect possibly adverse effects on said test system *(col. 4, lines 57-60; col. 6, lines 30-36; col. 10, lines 11-34; Fig. 11; wherein at least steps 930, 970, and 990-1010)*; and

i) in the presence of an adverse effect, blocking, by said test system, the communication entities leading to said adverse effect *(col. 10, lines 19-34; Fig. 11; step 970: 'block connection')*, and

ii) in the absence of an adverse effect, allowing, by said test system, the communication entities not having the adverse effect to communicate with said set of machines *(col. 6, lines 50-59; if it does, this is an indication that intruder may be attempting to breach the private network by masquerading as a trusted hot; in this case, the screen 340 should drop the packet without reply [i.e., otherwise, the screen will not drop the packet (forwarding the packet to destination)]; col. 7, lines 16-21; col. 7, lines 39-43; col. 10, lines 19-34; Fig. 11; steps 990: 'create connection' and 1010: 'check connection')*.

- **Regarding claim 38**, Baehr discloses the method of claim 37, wherein said at least part of said communication entities directed toward said test system include communication entities from traffic bound toward said set of machines *(col. 4, lines 57-60; col. 6, lines 30-36; Figs. 4-7)*.

- **Regarding claim 39**, Baehr discloses the method of claim 37, wherein said at least part of said communication entities directed toward said test system include communication entities from traffic coming from said set of machines *(col. 4, lines 41-49; Figs. 4-7)*.

- **Regarding claim 46**, Baehr discloses the method of claim 37, comprising, in the presence of said adverse effect, the step of subjecting to a resetting step those of said test facilities in said test system affected by said adverse effect *(col. 6, lines 37-67 to col. 7, lines 1-7; packet is either blocked or allowed depending on predetermined criteria and/or predefined table)*.

- **Regarding claim 47**, Baehr discloses the method of claim 37, wherein the machines in said set comprise facilities exposed to said adverse effect as well as additional contents, comprising the step of configuring said test facilities in order to replicate said facilities exposed to said adverse effect in the machines in said set *(col. 6, lines 37-59; col. 7, lines 55-63; packets, especially failed attempts or requests, are logged in the log file storage 640)*.

- **Regarding claim 48**, Baehr discloses the method of claim 37, comprising the step of inhibiting said test machines in said test system from providing responses to said traffic *(col. 7, lines 16-24; packets from any other source will be dropped without further action)*.

- **Regarding claim 49**, Baehr discloses the method of claim 37, comprising the steps of:

providing an in-line component ensuring said traffic with said set of machines *(col. 3, lines 59-64; Figs. 5-9; packet screening system 340 and network interface 1)*; and

providing at least one interface interfacing said in-line component with said test system *(col. 3, lines 59-64; Figs. 5-9; packet screening system 340 and network interface 2)*.

- **Regarding claim 50**, Baehr discloses the method of claim 49, comprising the step of providing feedback from said test system to said in-line component via said at least one interface *(col. 4, lines 33-67 to col. 5, lines 1-14; Fig. 5-7; screening system 340, network interface 2, and proxy network 430)*.

- **Regarding claim 51**, Baehr discloses the method of claim 49, comprising the steps of:

providing a management network for managing said test system *(col. 7, lines 13-24; administrator is ale to select security protocol and predefined criteria for packet filtering/processing)*; and

providing feedback from said test system to said in-line component via said management network *(col. 7, lines 13-24; administrator is ale to select security protocol and predefined criteria for packet filtering/processing)*.

- **Regarding claims 54-56**, claims 54-56 are similar in scope to claims 37-39 respectively, and are therefore rejected under similar rationale.

- **Regarding claims 63-68**, claims 63-68 are similar in scope to claims 46-51 respectively, and are therefore rejected under similar rationale.

- **Regarding claim 71**, claim 71 is similar in scope to claim 54 and is therefore rejected under similar rationale.

- **Regarding claim 72**, claim 72 is similar in scope to claim 37 and is therefore rejected under similar rationale.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

13. **Claims 40-45, 52-53, 57-62, and 69-70 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Baehr, as applied to claim 37 above, in view of Ramsey et al., (hereinafter "Ramsey"), U.S. Patent No. 7,331,061, filed on September 07, 2001.

- **Regarding claim 40**, Baehr discloses the method of claim 37.

Baehr does not explicitly discloses providing a data base comprising patterns representative of forbidden communication entities for communication with said set of machines; and blocking forbidden communication entities in said traffic as identified by respective patterns included in said data base.

However, in an analogous art, Ramsey discloses an integrated computer security management method including steps of providing a data base comprising patterns representative of forbidden communication entities for communication with said set of machines *(Ramsey: col. 3, lines 35-38; col. 4, lines 43-49; col. 5, lines 38-47; col. 18, lines 29-55; Fig. 5, wherein at least steps 542: signature match? Y/N and profile match: Y/N)*; and blocking forbidden communication entities in said traffic as identified by respective patterns included in said data base *(Ramsey: col. 3, lines 35-38; col. 4, lines 43-49; col. 5, lines 38-47; col. 17, lines 20-35; Fig. 5; wherein at least steps 514/528/652: deny/reject? Y/N)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Ramsey with the method and system of Baehr to include steps of providing a data base comprising patterns representative of forbidden communication entities for communication with said set of

machines; and blocking forbidden communication entities in said traffic as identified by respective patterns included in said data base to provide user with a means for managing security information with parallel processing, serial processing, or singular processing by a firewall, and IDS, and an AVS *(Ramsey: col. 2, lines 63-67)*.

- **Regarding claim 41**, Baehr discloses the method of claim 37.

Baehr does not explicitly disclose providing a further data base comprising patterns representative of allowed communication entities for communication with said set of machines; and allowing communication of allowed communication entities in said traffic as identified by respective patterns included in said further data base.

However, in an analogous art, Ramsey discloses an integrated computer security management method including steps of providing a further data base comprising patterns representative of allowed communication entities for communication with said set of machines *(Ramsey: col. 3, lines 35-38; col. 4, lines 43-49; col. 5, lines 38-47; col. 18, lines 29-55; Fig. 5, wherein at least steps 538: compare packet/copy to IDS signature and 542: signature match? Y/N and profile match: Y/N)*; and allowing communication of allowed communication entities in said traffic as identified by respective patterns included in said further data base *(Ramsey: col. 3, lines 35-38; col. 4, lines 43-49; col. 5, lines 38-47; col. 17, lines 20-35; Fig. 5; wherein at least steps : compare packet/copy to IDS signature; 552: trust? Y/N and 514/528/652: deny/reject? Y/N)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Ramsey with the method and

system of Baehr to include steps of providing a further data base comprising patterns representative of allowed communication entities for communication with said set of machines; and allowing communication of allowed communication entities in said traffic as identified by respective patterns included in said further data base to provide user with a means for managing security information with parallel processing, serial processing, or singular processing by a firewall, and IDS, and an AVS *(Ramsey: col. 2, lines 63-67)*.

- **Regarding claim 42**, Baehr and Ramsey disclose the method of claim 40.

Baehr and Ramsey further disclose detecting unknown communication entities in said traffic as identified by respective unknown patterns not included in said data base *(Baehr: col. 7, lines 13-29; packages from (or to) any other source (unknown source) will be dropped; Ramsey: Fig. 5; wherein at least step 542: 'profile match? Y/N')*; and directing said unknown communication entities in said traffic as identified by respective unknown patterns not included in said data base toward said test system to be run on said test facilities to detect possibly adverse effects on said test system *(Baehr: col. 4, lines 57-60; Figs. 4-7; requests from public network will be forwarded to proxy network; see also col. 6, lines 30-36; Ramsey: Fig. 5; wherein at least step 542: 'profile match? Y/N')*.

- **Regarding claim 43**, Baehr and Ramsey disclose the method of claim 42.

Baehr further discloses in the presence of said adverse effect, the step of adding to said data base the respective pattern identifying the communication entity leading to said adverse effect *(Baehr: col. 6, lines 37-59; col. 7, lines 55-63; packets, especially failed attempts or requests, are logged in the log file storage 640)*.

- **Regarding claim 44**, Baehr and Ramsey disclose the method of claim 41.

Baehr and Ramsey further disclose detecting unknown communication entities in said traffic as identified by respective unknown patterns not included in said further data base *(Baehr: col. 7, lines 13-29; unknown packets are determined by predetermined criteria; Ramsey: Fig. 5; wherein at least steps 512 and 552: determine if packet is trusted? Y/N)*; and

directing said unknown communication entities in said traffic as identified by respective unknown patterns not included in said further data base toward said test system to be run on said test facilities to detect possibly adverse effects on said test system *(Baehr: col. 4, lines 57-60; Figs. 4-7; requests from public network will be forwarded to proxy network; see also col. 6, lines 30-36)*.

- **Regarding claim 45**, Baehr and Ramsey disclose the method of claim 44.

Baehr and Ramsey further disclose in the absence of said adverse effect, the step of adding to said further data base the respective pattern identifying the communication entity failing to lead to said adverse effect *(Baehr: col. 7, lines 13-29; unknown packets are determined by predetermined criteria; Ramsey: col. 12, lines 63-67 to col. 13, lines 1-3; updating IDS configuration and/or signature files)*.

- **Regarding claim 52**, Baehr and Ramsey disclose the method of claim 43.

Ramsey further discloses providing a parallel intrusion preventing arrangement including a respective data base including patterns representative of respective forbidden communication entities for communication with a respective set of machines *(Ramsey: col.*

16, lines 23-30; parallel processing occurs where the IDS 255 processes the copied packet while the actual packet is processed by the firewall 225); and

in the presence of said adverse effect, transmitting to said parallel intrusion preventing arrangement, for inclusion in said respective data base, the respective pattern identifying the communication entity leading to said adverse effect *(Ramsey: col. 16, lines 23-60; decision step 512, it is determined whether a packet is 'trusted')*.

- **Regarding claim 53**, Baehr and Ramsey disclose the method of claim 45.

Ramsey further discloses providing a parallel intrusion preventing arrangement including a respective further data base including patterns representative of respective allowed communication entities for communication with a respective set of machines *(Ramsey: col. 16, lines 23-30; col. 19, lines 8-34; parallel processing occurs where the IDS 255 processes the copied packet while the actual packet is processed by the firewall 225)*; and

in the absence of said adverse effect, transmitting to said parallel intrusion preventing arrangement, for inclusion in said respective further data base, the respective pattern identifying the communication entity failing to lead to said adverse effect *(Ramsey: col. 16, lines 23-60; col. 19, lines 8-34; decision step 512, it is determined whether a packet is 'trusted')*.

- **Regarding claims 57-62**, claims 57-62 are similar in scope to claims 40-45 respectively, and are therefore rejected under similar rationale.

- **Regarding claims 69-70**, claims 69-70 are similar in scope to claims 52-53 respectively, and are therefore rejected under similar rationale.

Conclusion

14. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luu Pham whose telephone number is 571-270-5002. The examiner can normally be reached on Monday through Friday, 7:30 AM - 5:00 PM (EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Luu Pham/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437